



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/656,439	09/05/2003	Diana K. Smetters	PARC-DA3162	8476
35699 7590 10/30/2007 PVF -- PARC c/o PARK, VAUGHAN & FLEMING LLP 2820 FIFTH STREET DAVIS, CA 95618-7759			EXAMINER LEMMMA, SAMSON B	
			ART UNIT 2132	PAPER NUMBER
			MAIL DATE 10/30/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/656,439

Applicant(s)

SMETTERS ET AL.

Examiner

Samson B. Lemma

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 15 August 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-4, 6-13, 15-22 and 24-30 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-4, 6-13, 15-22 and 24-30 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____

- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

1. This office action is in reply to an amendment filed on August 15, 2007.
Claims 5, 14 and 23 are previously been canceled. No new claims are added. Thus claims 1-4, 6-13, 15-22 and 24-30 are pending/examined.
2. In the previous office action, the office rejected **independent Claims 1, 10 and 19** under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. Examiner pointed out that the specification/original disclosure fails to mention/specify or teach the negative limitation, which was previously added in every independent claims 1,10 and 19, namely "**wherein the preferred channel does not require being resistant to eavesdropping.**"
Thus the above negative limitation was considered/found to be a new matter by the office. However Applicant's representative argument overcomes this rejection and the rejection is withdrawn. The following office action is written in view of the argument presented and applicant's specification written on paragraph 0078.

Priority

3. This application claims priority of a provisional application 60/480,909 filed on June 24, 2003. Therefore, the effective filing data for the subject matter defined in the pending claims of this application is **06/24/2003**.

Response to Arguments

4. Applicant's remark/arguments filed on August 15, 2007 regarding have been fully considered but are moot in view of new ground (s) of rejection.

Art Unit: 2132

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. **Claims 1-4, 6-13, 15-22 and 24-30** are rejected under 35 U.S.C. 103(a) unpatentable over **Hermann, Reto** (hereinafter referred as **Hermann**) (European Patent Publication No. EP1024626A1) (Publication Date 08/02/2000) (Submitted with the Applicant's IDS) in view of Stirbu (hereinafter referred as **Stirbu**) (U.S. Publication No. 2003/0200431) (filed on: April 18, 2002)

Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

7. **As per independent claims 1, 10 and 19** Hermann discloses a computer controlled method comprising:

- **Establishing communication between a situation notification device [see , paragraph 0020, "first device"] and a provisioning device [see , paragraph 0020, "second device/servicing device"] over a preferred channel [See, paragraph 0020, "communication link"];[paragraph 0020, lines 15-21]**

Art Unit: 2132

- **Providing provisioning information to said situation notification device over said preferred channel,**[Paragraph 0020, lines 44-48] *(After receiving the sequence, the serving device responds by sending back over a wireless broadcast medium a respond. And as it is disclosed on paragraph 0020, lines 44-48 such responds may comprises, a key, also a session key and a communication parameters which meets the limitation of provisioning information from serving device to personal device/situation notification for further communication. In other words the personal device/situation notification device is provided with key, session key and a communication parameters/provisioning information)*

wherein said situation notification device is automatically configured to receive subject matter information responsive to said provisioning information; [Paragraph 0020, lines 48-49] *(And the situation notification device is automatically configured to receive the encrypted information which meets the limitation of the subject matter information)*

- **Receiving said subject matter information;** [Paragraph 0020, lines 48-49] *(encrypted information)*
- **Verifying said subject matter information with said provisioning information;** [Paragraph 0014] *(Only the intended receiver/notification device receives the encrypted subject matter since it is the one that has the corresponding decryption key and the encrypted information/subject matter information with the corresponding private key/public key/session key/provisioning information are decrypted and verified that the subject matter is sent form the right provisioning device.)*

Art Unit: 2132

- **Presenting said subject matter information to a user of the situation notification device responsive to the step of verifying, wherein the step of verifying ensures that the subject matter information is genuine..** [Paragraph 0014 & abstract] *(Only the intended receiver/notification device receives the encrypted subject matter since it is the one that has the corresponding decryption key. And the encrypted information/subject matter information is presented to a user of the situation notification device only and only if the situation notification device carries the corresponding private key/public key/session key/provisioning information and successfully decrypts and verifies that the subject matter is sent from the right provisioning device, by doing so the situation notification device ensures that the subject matter information is genuine. This is simply another application of public key cryptography, explained on paragraph 0014 and secure transmission disclosed in the abstract.)*

Hermann does not explicitly disclose the limitation recited as **"wherein the preferred channel does not require being resistant to eavesdropping."**

However, in the same field of endeavor **Stirbu on paragraph 0008**, discloses that a TLS Handshake Protocol allows a server and client in a communication session to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data. The TLS Handshake Protocol provides connection security having three basic properties: the peer's identity can be authenticated using asymmetric, or public key, cryptography (e.g., RSA, DSS, etc.); the negotiation of a shared secret is

Art Unit: 2132

secure in that the **negotiated secret is unavailable to eavesdroppers**, and for any authenticated connection **the secret cannot be obtained**, even by an attacker who can place himself in the middle of the connection; **and the negotiation is reliable in that no attacker can modify the negotiation communication without being detected by the parties to the communication.**

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the feature of which a channel does not need to be resistant to eavesdroppers to be used as a preferred channel because only public information (e.g., a public key, or a commitment to a public key) is sent over that channel; a pair of devices authenticating themselves to each other by sending such key or commitment information over the preferred channel are able to set up a secure communication with each other because they can demonstrate possession of the private keys corresponding to the public keys and eavesdropper that detects the commitment or keys sent across the preferred channel is not able to demonstrate possession of the corresponding private key as per teachings of **Stirbu** in to the method as taught **Hermann** in order to build a trust infrastructures. [See Stirbu, paragraph 0003]

8. **As per claims 2, 11 and 20 the combination of Hermann and Stirbu** discloses a computer controlled method as applied to claims above. Furthermore, **Hermann discloses a method, wherein the step of providing further comprises:**
- exchanging key commitment information over said preferred channel between said provisioning device and said situation notification device;** [paragraph 0020]

Art Unit: 2132

receiving a public key by said situation notification device; [paragraph 0021, line 39] verifying said public key with said key commitment information [Paragraph 0021, lines 41-42] [the serving device, inherently verifies the password or the public key sent by the personal device before responding to the personal device. After verification, the service device sends back a communication parameters for further communication to the personal device]; and receiving a credential authorized by a credential issuing authority. [paragraph 0022]

9. As per claims 3, 12 and 21 the combination of Hermann and Stirbu discloses a computer controlled method as applied to claims above. Furthermore, Hermann discloses a method, wherein said preferred channel is a location-limited channel. [paragraph 0020, lines 20-21]

10. As per claims 4, 13 and 22 the combination of Hermann and Stirbu discloses a computer controlled method as applied to claims above. Furthermore, Hermann discloses a method, wherein, wherein said preferred channel uses a telephone switching system. [paragraph 0025-0026 and 0041-0042]

11. As per claims 6, 15 and 24 the combination of Hermann and Stirbu discloses a computer controlled method as applied to claims above. Furthermore, Hermann discloses a method, wherein subject matter information is received using an antenna, a telephone line, a local area network, a wide area network, a wireless network, or a broadcast network. [paragraph 0041-0042]

12. As per claims 7, 16 and 25 the combination of Hermann and Stirbu discloses a computer controlled method as applied to claims above. Furthermore, Hermann discloses a method, wherein said situation notification device is a

Art Unit: 2132

computer, a television, a radio, a telephone, a push to talk device, a pager, a clock, a thermostat, a network appliance, or a home appliance. [paragraph 0039]

13. As per claims 8-9, 17-18 and 26-27 the combination of Hermann and Stirbu discloses a computer controlled method as applied to claims above. Furthermore, Hermann discloses a method, further comprising forwarding said subject matter information, wherein said subject matter information is alarm information. [Paragraph 0039, lines 44-46]

14. As per claims 28-30 the combination of Hermann and Stirbu discloses a computer controlled method as applied to claims above. Furthermore, Hermann discloses a method, wherein said preferred channel has a demonstrative identification property and an authenticity property.

[paragraph 0027] (The limitation recited in the amended independent claims as the preferred channel has "demonstrative identification property" is defined as follows in applicant's specification, (see publication no. 20040268119, paragraph 0054, the last sentence), "The demonstrative identification property of the preferred channel means that human operators are aware of which devices are communicating with each other over the preferred channel and that the human operators can easily detect when an attack is being made on the preferred channel."

Furthermore, the limitation recited in the amended independent claims as the preferred channel has "an authenticity property" is defined as follows in applicant's specification, (see publication no. 20040268119, paragraph 0055) "The authenticity property of the preferred channel means that it is impossible or difficult for an attacker to transmit over the preferred channel or tamper with messages sent over the preferred channel without detection by the legitimate parties to the communication."

Art Unit: 2132

Examiner would like to point out that the reference on the record, namely Hermann discloses such concepts/limitation as shown below which meets the recitation the amended limitation.

Hermann on paragraph 0026 discloses that initiating the communication session and for transmitting an initial-sequence that may contain sensitive information, the unidirectional wireless communication channel can ensure that only the target device receives the initial-sequence. It is especially advantageous if a directed channel as line-of-sight link can be used, because than no other parties can eavesdrop and receive the initial-sequence. Such a channel can be an optical channel, e.g. an infrared or a laser channel, a Personal Area Network (PAN) channel, a directed radio-frequency (RF) channel, an inductive channel, a capacitive channel, or every other channel that is suitable for low-range, directed communication links.

Furthermore Hermann on paragraph 0029, discloses that it is very simple to set up a communication if the personal device is connected to a user, e.g. by a PAN, because the user touches then in an intuitive way the serving device for initiating the unidirectional wireless communication channel via his body. There are no additional cards or other things necessary for setting up an authenticated session. The above paragraphs such as paragraph 0026 & 0029 recited on the record implies the fact that "when attack is being made on the preferred channel it can easily detected"and meets the limitation recited as " the preferred channel has "demonstrative identification property" Likewise, Hermann on paragraph 0030, discloses that if the response as well as the further communication over the wireless broadcast medium is protected by using a cryptosystem, than the advantage occurs, that the exchanged information is hidden perfectly and can not be uncovered by someone else. A suitable system can be a public-key cryptosystem where only the public key is exchanged once. Furthermore, what is

recited on paragraph 0026 in combination with the "authenticated session" or "protected by using a cryptosystem" disclosed on paragraph 0026 and 0029, meets the limitation that "the preferred channel has "an authenticity property". Furthermore, Stirbu on paragraph 0008, discloses that a TLS Handshake Protocol allows a server and client in a communication session to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data. The TLS Handshake Protocol provides connection security having three basic properties: the peer's identity can be authenticated using asymmetric, or public key, cryptography (e.g., RSA, DSS, etc.); the negotiation of a shared secret is secure in that the negotiated secret is unavailable to eavesdroppers, and for any authenticated connection the secret cannot be obtained, even by an attacker who can place himself in the middle of the connection; and the negotiation is reliable in that no attacker can modify the negotiation communication without being detected by the parties to the communication.)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-873-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status

Art Unit: 2132

information for unpublished applications is available through Private PAIR only.

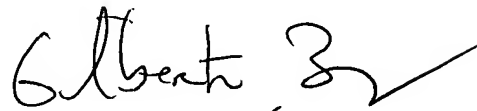
For more information about the PAIR system, see <http://pair-direct.uspto.gov>.

Should you have questions on access to the Private PAIR system, contact the

Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA

S.L.
10/20/2007

A handwritten signature in black ink, appearing to read "Gilberto Jr.", followed by a checkmark.

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100